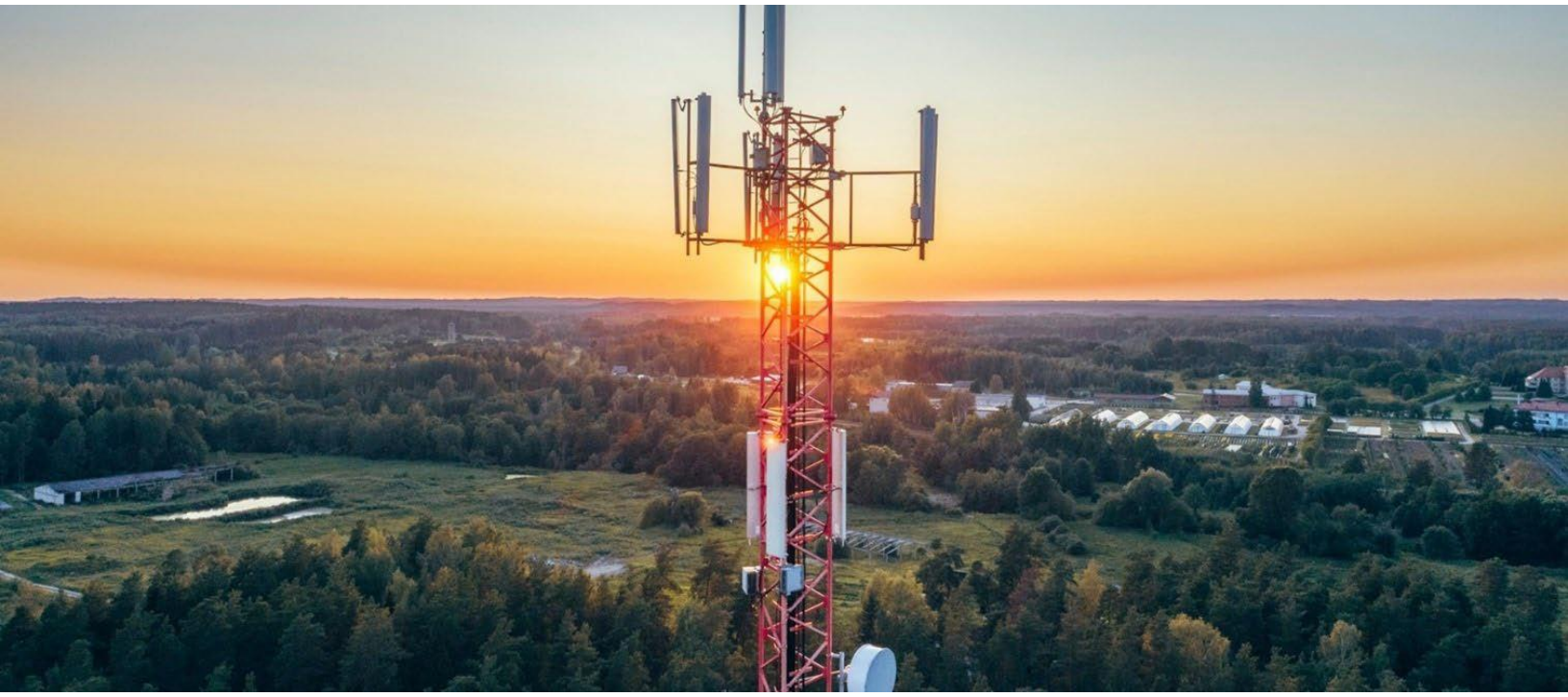
GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

National Cyber Security Centre
PART OF THE GCSB

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité



ENFOQUES MODERNOS PARA LA SEGURIDAD DEL ACCESO A LA RED

Publicación: 18 de junio de 2024

Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (U.S. Cybersecurity and Infrastructure Security Agency)

Oficina Federal de Investigaciones de EE. UU. (U.S. Federal Bureau of Investigation)

Oficina de Seguridad de las Comunicaciones del Gobierno de Nueva Zelanda (New Zealand's Government Communications Security Bureau)

Equipo de Respuesta a Emergencias Informáticas de Nueva Zelanda (New Zealand's Computer Emergency Response Team)

Centro Canadiense de Ciberseguridad (Canadian Centre for Cyber Security)

Índice

DESCRIPCIÓN GENERAL

La Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) ha identificado con frecuencia soluciones de redes privadas virtuales (VPN, por sus siglas en inglés) que han estado involucradas en muchos incidentes recientes de alto perfil, tanto con ciberdelincuentes como con agentes de estados-nación. La CISA ha descubierto más de 22 vulnerabilidades explotadas conocidas (KEV, por sus siglas en inglés) relacionadas con la vulneración de VPN, lo que conduce a un amplio acceso a las redes de las víctimas. Estos incidentes y vulnerabilidades asociadas están impulsando a algunos a considerar reemplazar sus soluciones VPN tradicionales con soluciones modernas de acceso a la red. El traslado de más servicios a la nube también destaca el valor de Secure Access Service Edge (SASE) en lugar de una pila de seguridad tradicional ubicada en un centro de datos local. Si bien algunas soluciones VPN son por naturaleza más seguras que otras (y no siempre son la causa de incidentes cibernéticos importantes), las redes híbridas actuales requieren la adopción de soluciones modernas de seguridad de acceso a la red para ayudar a las organizaciones a proteger los recursos corporativos. Además, estas soluciones de acceso a la red brindan oportunidades para integrar un control de acceso granular que no es inherente a los enfoques VPN tradicionales. La CISA fomenta un análisis cuidadoso de cómo han cambiado sus necesidades de seguridad a la luz del mayor uso de los servicios en la nube y el aprovechamiento de cualquier actualización tecnológica para progresar en su camino hacia la Confianza Cero.

Las organizaciones que adopten estas nuevas prácticas alcanzarán un resultado general más cercano a los principios de confianza cero (ZT, por sus siglas en inglés).

Este informe proporciona una descripción general de los enfoques modernos de seguridad de acceso a la red para líderes ejecutivos, defensores de redes de infraestructura crítica y organizaciones gubernamentales. El informe está destinado en concreto a las organizaciones que desean pasar de las tradicionales implementaciones de acceso remoto generalizado a soluciones de seguridad más sólidas y detalladas (es decir, Secure Service Edge [SSE] y Secure Access Service Edge [SASE]). Al utilizar políticas de control de acceso basadas en riesgos para tomar decisiones a través de motores de decisiones de políticas, estas soluciones integran seguridad y control de acceso, lo que fortalece la usabilidad y la seguridad de una organización a través de políticas adaptativas. Este informe proporciona las mejores prácticas para usuarios y organizaciones que realizan la transición de arquitecturas tradicionales a la nube y proporciona principalmente soluciones basadas en la nube que pueden soportar implementaciones híbridas y locales en pos de objetivos de confianza cero.

También describe las protecciones para las redes de IT y tecnología operativa (OT, por sus siglas en inglés) en un espectro de sensibilidades de red y las peores consecuencias de una vulneración. La CISA, la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés), la Oficina de Seguridad de las Comunicaciones (GCSB, por sus siglas en inglés) del Gobierno de Nueva Zelanda, el Equipo de Respuesta a Emergencias Informáticas de Nueva Zelanda (CERT-NZ, por sus siglas en inglés) y el Centro Canadiense de Seguridad Cibernética (CCCS, por sus siglas en inglés) (en adelante, las organizaciones autoras) instan a los propietarios de empresas, sin importar su tamaño, a revisar este informe para comprender mejor las vulnerabilidades, amenazas y prácticas asociadas con el acceso remoto tradicional y la implementación de VPN, junto con el riesgo comercial inherente que representa para la red de una organización la configuración incorrecta del acceso remoto. Las organizaciones autoras publican este informe para brindar a los líderes orientación para ayudar a priorizar la protección de la seguridad del entorno informático remoto de las organizaciones mientras operan bajo los principios fundamentales del mínimo privilegio.

ACCESO REMOTO Y LIMITACIONES DE VPN

Una VPN de acceso remoto empresarial permite a los usuarios acceder a la red corporativa/comercial a través de un túnel privado y encriptado. Las VPN brindan a los empleados fácil acceso a servidores, aplicaciones de la empresa y datos externos. A pesar de esto, una vez que un usuario establece una conexión a través de una VPN para acceder a recursos en la red interna de la empresa, la organización puede ser susceptible a verse comprometida a través de varias limitaciones de la VPN, incluidas vulnerabilidades inherentes al diseño de la red (p. ej., dirección IP y suplantación de identidad del sistema de nombres de dominio [DNS, por sus siglas en inglés]), la complejidad de la implementación, una configuración incorrecta o incluso una vulnerabilidad en la solución de VPN.

Además de los riesgos generales de la VPN y el acceso remoto, los terceros que se conectan a la red de una organización también pueden representar riesgos debido a dispositivos comprometidos en la red y malas prácticas de higiene cibernética. Sin una segmentación estricta de la red y la adhesión a los principios de mínimo privilegio y confianza cero, las organizaciones que brindan acceso remoto a proveedores externos introducen riesgos adicionales a su entorno. Si bien algunas VPN se pueden configurar para aplicar políticas de firewall granulares para proporcionar niveles limitados de acceso a los recursos de la empresa, no todos los proveedores de VPN ofrecen esta opción. Muchas soluciones de VPN se basan en software, lo que significa que el riesgo de que agentes de amenazas cibernéticas exploten vulnerabilidades del software puede resultar perjudicial para las operaciones comerciales. Como tal, los dueños de negocios también deberían considerar soluciones reforzadas con hardware.

IMPACTO

Las vulnerabilidades en los sistemas de VPN pueden provocar impactos sustanciales en las organizaciones si son explotadas por agentes de amenazas porque pueden permitir un acceso fácil a través de una gran red empresarial después de la explotación exitosa del dispositivo. La CISA documentó múltiples vulnerabilidades de este tipo durante los últimos seis meses:

- CVE-2023-46805, CVE-2024-21887 y CVE-2024-21893 que afectan a las puertas de enlace Ivanti Connect Secure (ICS) e Ivanti Policy Secure. Varias fuentes observaron que el dispositivo VPN ICS con conexión a Internet fue víctima de un ataque cuando un atacante explotó datos de configuración para realizar un túnel inverso desde el dispositivo VPN ICS.[1] Luego, el atacante modificó un archivo JavaScript utilizado por el componente Web VPN SSL del dispositivo para comprometer las credenciales y pasar de un sistema a otro.[1] Durante el análisis forense se utilizaron datos forenses de memoria y disco, combinados con la herramienta Integrity Checker, para identificar archivos maliciosos en el dispositivo VPN Ivanti Connect Secure comprometido.[2] Sin embargo, esta herramienta y el parche no lograron detectar la vulneración debido a que los agentes de amenazas prácticamente no fueron detectados, eludieron el restablecimiento de fábrica y obtuvieron acceso a nivel de raíz.[2]
- CVE-2023-4966 (Citrix Bleed) que afecta al control de entrega de aplicaciones web (ADC, por sus siglas en inglés) de Citrix NetScaler y a los dispositivos NetScaler Gateway. Esta vulnerabilidad permitió a los agentes de amenazas eludir los requisitos de contraseña y la autenticación multifactor (MFA, por sus siglas en inglés), lo que permitió el secuestro exitoso de sesiones de usuarios legítimos en aplicaciones web de Citrix NetScaler. Al secuestrar sesiones de usuarios legítimos, los agentes de amenazas adquirieron permisos elevados para recolectar credenciales, moverse lateralmente y acceder a datos y recursos.[3] Los afiliados de Lockbit 3.0 explotaron esta vulnerabilidad en ataques de ransomware.[3]

Además de explotar vulnerabilidades, los agentes de amenazas pueden obtener acceso a todos los servicios dentro de la red de una organización si utilizan un dispositivo o una cuenta comprometidos y se conectan a través de servicios de VPN. Los riesgos más importantes para las entidades de infraestructura crítica son aquellos que utilizan una VPN vinculada a la gestión de identidad y Active Directory. Como se señala en un aviso conjunto, Agentes patrocinados por el estado de la PCR (República Popular China) comprometen y mantienen un acceso persistente en las infraestructuras críticas de los EE. UU., Volt Typhoon, un grupo cibernético patrocinado por el Estado de la PCR que ataca infraestructura crítica de EE. UU., utiliza sesiones de VPN para conectarse de forma segura a entornos de víctimas con credenciales administrativas. Esto permite a los agentes de Volt Typhoon moverse lateralmente, obtener credenciales de dominio para la red y mezclarse con el tráfico regular, reduciendo de forma significativa su riesgo de detección.

SOLUCIONES

Las soluciones modernas actuales (confianza cero, SSE y SASE) brindan acceso remoto a aplicaciones y servicios según una política de control de acceso granular. Este tipo de política rechaza el acceso a usuarios que no estén explícitamente autenticados y autorizados para una aplicación o servicio en particular. Consulte las secciones siguientes para obtener más detalles. Las organizaciones pueden adoptar un enfoque más seguro para el acceso a la red mediante la implementación de los principios ZT y el monitoreo continuo de la actividad del usuario, lo que promueve la seguridad de los datos en tránsito. Al no exponer las aplicaciones internas a riesgos innecesarios, la organización puede reducir la amenaza general de vulneración, lo que protege aún más los datos en reposo. La eficacia de cualquier solución de seguridad moderna propuesta depende en gran medida de cómo esté diseñada la red y la infraestructura de la organización. Adherirse a los principios de ZT en cualquier grado mejorará la capacidad de la organización para proteger la información al mantenerla a salvo de amenazas y pérdida de datos. Las soluciones modernas actuales (arquitectura ZT, SSE y SASE) cumplen con los principios de ZT y brindan acceso remoto a aplicaciones y servicios según una política de control de acceso granular.

Nota: Las organizaciones pueden diferir entre sí, y cada solución tiene necesidades únicas de planificación, arquitectura o adaptación. Las organizaciones deben evaluar sus necesidades y su postura de seguridad y tomar una decisión informada basada en un análisis exhaustivo antes de seleccionar una solución.

CONFIANZA CERO

La confianza cero (ZT), definida por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) en la Publicación Especial (SP, por sus siglas en inglés) 800-207, está diseñada para evitar el acceso no autorizado a datos y servicios junto con la aplicación de un control de acceso granular. La ZT es una colección de conceptos e ideas que ayudan a las organizaciones a implementar decisiones de acceso precisas por solicitud basadas en los principios del mínimo privilegio en los sistemas y servicios de información. Opera bajo el supuesto de que no se debe confiar de forma implícita en ningún usuario o activo, lo que requiere que cada usuario, dispositivo y aplicación se vuelva a autenticar y autorizar continuamente durante toda la transacción.

Para desarrollar estrategias de confianza cero y planes de implementación, las organizaciones deben adoptar el Modelo de Optimización de Confianza Cero (ZTMM, por sus siglas en inglés) de la CISA. El ZTMM representa una gradiente de implementación a través de cinco pilares distintos, en los que, con el tiempo, se pueden realizar avances menores hacia la optimización. El modelo también presenta formas en que varios programas de ciberseguridad de la CISA apoyan las soluciones de ZT.

Nota: La CISA y las organizaciones autoras animan a todas las organizaciones a revisar las políticas, los procedimientos y las publicaciones de confianza cero según lo define su centro de ciberseguridad principal al desarrollar un plan de acción e implementación.

Para obtener más información sobre la confianza cero y el modelo de optimización de confianza cero, consulte el Modelo de optimización de confianza cero de la CISA.

SECURE SERVICE EDGE

SSE es una colección de capacidades de seguridad en la nube que permiten una navegación segura, una aplicación de software como servicio (SaaS, por sus siglas en inglés) más segura y un enfoque sencillo para validar a los usuarios que acceden a los datos de la red. Además, SSE es un enfoque integral de la seguridad de la red, que combina redes, prácticas y políticas de seguridad y servicios en una única plataforma. Este enfoque permite a las organizaciones garantizar la seguridad de las aplicaciones y el acceso a los datos sin importar el dispositivo o la ubicación del usuario. Las capacidades de seguridad de SSE consisten en acceso a la red de confianza cero, puerta de enlace web segura en la nube, agente de seguridad de acceso a la nube y firewall como servicio.[4]

Acceso a la red de confianza cero

Acceso a la red de confianza cero (ZTNA, por sus siglas en inglés) es una solución de seguridad de IT diseñada para proporcionar acceso remoto más seguro a las aplicaciones, los datos y los servicios de una organización al operar con políticas de control de acceso estrictamente definidas. Estas políticas se adhieren a los principios de confianza cero y facilitan la seguridad durante el acceso remoto mediante la implementación de metodologías de control de acceso de confianza cero y otorgando acceso con el mínimo privilegio. A través del ZTNA, las organizaciones pueden restringir las herramientas disponibles para posibles atacantes que obtengan acceso a dispositivos o servicios remotos comprometidos. Esto se logra mediante un agente de seguridad de acceso, que verifica la identidad del usuario, los requisitos de acceso y las reglas de política de confianza cero. Los agentes de seguridad también pueden monitorear las conexiones, incluida la postura de seguridad del dispositivo y la geolocalización del cliente, y aplicar MFA. Los usuarios se someten a una nueva autenticación periódica durante cada sesión para garantizar la seguridad y la identificación. El proceso de autenticación se reinicia por completo si los usuarios buscan acceso a aplicaciones adicionales.

Puerta de enlace web segura en la nube

Puerta de enlace web segura (SWG, por sus siglas en inglés) en la nube es una solución de seguridad que protege a los usuarios y dispositivos de las amenazas basadas en la web y aplica políticas de seguridad dentro de la red. La SWG actúa como un filtro de URL entre los usuarios e Internet. Es un método de detección de contenido malicioso o no autorizado, controles de acceso web, descifrado de capa de sockets seguros/seguridad de la capa de transporte (SSL/TLS, por sus siglas en inglés) para análisis de tráfico cifrado, control de aplicaciones, autenticación de usuarios y análisis de informes.

Agente de seguridad de acceso a la nube

El agente de seguridad de acceso a la nube (CASB, por sus siglas en inglés) es una solución de seguridad en la nube que puede ayudar a las organizaciones a administrar datos en múltiples aplicaciones de software como servicio, así como cuando los datos están en tránsito hacia entornos de nube. Un CASB también puede ayudar a las organizaciones a aplicar políticas de seguridad, gobernanza y cumplimiento, detectar y mitigar amenazas a la nube y habilitar la capacidad de una organización para garantizar la protección efectiva de los datos en múltiples ubicaciones.

Firewall como servicio

Firewall como servicio (FWaaS, por sus siglas en inglés) es una solución de seguridad basada en la nube que permite a las organizaciones monitorear y agregar tráfico de múltiples fuentes, como centros de datos, oficinas e infraestructuras en la nube. FWaaS funciona de manera similar a un firewall tradicional; inspecciona y filtra el tráfico de red, aplica políticas y protege contra amenazas cibernéticas. Con la integración de FWaaS, las organizaciones tienen la capacidad de administrar de forma centralizada a través de un panel basado en la nube, lo que promueve la escalabilidad, la flexibilidad y la administración simplificada.

SECURE ACCESS SERVICE EDGE

Mientras que SSE opera mediante la convergencia de funciones de seguridad en un único servicio en la nube, Secure Access Service Edge (SASE) es una arquitectura en la nube que combina la red y la seguridad como capacidad de servicio, incluida la red de área amplia definida por software (SD-WAN, por sus siglas en inglés), SWG, CASB, firewall de nueva generación (NGFW, por sus siglas en inglés) y ZTNA.[5] Los proveedores de servicios en la nube (CSP, por sus siglas en inglés) pueden proporcionar a las organizaciones redes y seguridad como servicio en lugar de implementar soluciones de seguridad en las instalaciones o ser dirigidos a centros de datos. Esto permite a los administradores de red tener visibilidad de todos los puertos, protocolos y aplicaciones proporcionados por el CSP o la organización. El modelo SASE ofrece una interfaz de gestión segura, reduce la complejidad e implementa dispositivos de seguridad que fomentan políticas sólidas y más seguras.

Red de área amplia definida por software

La red de área amplia definida por software (SD-WAN, por sus siglas en inglés) es una solución/tecnología ofrecida que simplifica la gestión y el funcionamiento de redes de área amplia (WAN, por sus siglas en inglés). En las configuraciones de WAN tradicionales, la gestión de la red está estrechamente ligada al hardware, como enrutadores y conmutadores. Con la SD-WAN, las organizaciones poseen la capacidad de abstraer la infraestructura de red, lo que permite el control y la gestión centralizados a través del software. Estas son las características principales de la SD-WAN:

- Control centralizado
- Integración de la seguridad
- Visibilidad y análisis

Cortafuegos de nueva generación

El cortafuegos de nueva generación (NGFW, por sus siglas en inglés) es un dispositivo de seguridad de red que realiza funciones de seguridad de firewall tradicionales al tiempo que posee capacidades de protección contra amenazas y vulnerabilidades. Además del filtrado de paquetes y la inspección de estado, el NGFW proporciona lo siguiente:

- La capacidad de permitir un control más granular sobre el tráfico de la red mediante la identificación y el control de aplicaciones, así como la supervisión de puertos y protocolos.
- Sistemas de prevención de intrusiones (IPS, por sus siglas en inglés) integrados diseñados para detectar y bloquear anomalías en las redes de la empresa.
- Protección avanzada contra amenazas y fuentes de inteligencia de amenazas integradas para mejorar la mitigación contra ataques dirigidos.
- Filtrado de contenido que inspecciona y filtra el contenido web (incluido el filtrado basado en URL y contenido) para aplicar políticas de ZT, detectar sitios web maliciosos y evitar la exfiltración de datos.

En una arquitectura SASE, el tráfico empresarial se puede enrutar a servicios basados en la nube de varias maneras según el proveedor. La SD-WAN se considera una de las formas más efectivas de enrutar el tráfico según los requisitos específicos de la organización. Ofrece selección de ruta dinámica, gestión centralizada e integración de seguridad. Las soluciones SASE brindan a las organizaciones un mayor control sobre los usuarios al clasificar el tráfico en la capa de aplicación y en toda la red y al limitar el acceso otorgado, los datos que pueden obtener los usuarios y las aplicaciones que se pueden usar mientras operan en un entorno empresarial. SASE también mejora el monitoreo continuo al utilizar una sola plataforma (en lugar de manejar el monitoreo y los informes en múltiples consolas). Esto permite una respuesta eficiente a incidentes y reduce la complejidad al optimizar la red y la seguridad. Al condensar las plataformas y eliminar las soluciones de seguridad puntuales que requieren un uso manual intensivo, SASE puede ayudar a reducir los desafíos logísticos asociados con el envío, la instalación y la actualización de dispositivos de red y seguridad.[5]

SASE proporciona seguridad más sencilla, mejor experiencia de usuario, seguridad de la interfaz de administración, implementación rápida y costos reducidos.

Segmentación de red reforzada por hardware

La segmentación de red reforzada por hardware se utiliza en redes donde las operaciones cibernéticas plantean amenazas creíbles a la seguridad pública, la seguridad nacional y las funciones críticas. Más en concreto, esta práctica agrega una capa de protección de hardware a una postura de seguridad de defensa en profundidad, abordando el riesgo generalizado de vulnerabilidades conocidas y desconocidas en las soluciones de seguridad basadas en software. La segmentación de red reforzada por hardware utiliza tecnologías unidireccionales, como puertas de enlace unidireccionales o diodos de datos (NIST SP800-82 revisión 3).

Estos son algunos ejemplos de acceso remoto que utilizan segmentación de red ejecutada por hardware:

- La vista de pantalla remota unidireccional transmite imágenes de pantalla en tiempo real a través de hardware unidireccional a técnicos de servicio remotos. Esos técnicos pueden luego proporcionar al personal en el lugar asesoramiento en tiempo real para diagnosticar y corregir problemas complejos.
- Los sistemas de acceso remoto, con canales de control de hardware unidireccionales para pulsaciones de teclas y movimientos del ratón, son independientes de los canales de monitoreo unidireccionales para imágenes de pantalla y brindan protecciones más fuertes que los sistemas que solo utilizan software.[6]

En ambos casos, puede ser apropiado implementar conmutadores de hardware con límite de tiempo que permitan un acceso remoto bidireccional temporal en paralelo con soluciones unidireccionales y en serie con soluciones de seguridad de acceso remoto basadas en software. Estos conmutadores de tiempo limitado brindan al personal en sitios protegidos control físico sobre cuánto tiempo está habilitado el acceso remoto basado en software.

PRÁCTICAS RECOMENDADAS

La segmentación de red reforzada por hardware, SASE y SSE brinda a las organizaciones la posibilidad de reemplazar las VPN y las funciones de seguridad tradicionales y fomentar políticas que ofrezcan un enfoque de confianza cero para la implementación de seguridad moderna. Las organizaciones autoras animan a todas las entidades a evaluar con atención su postura de seguridad y realizar un análisis de riesgos antes de implementar cualquier solución para determinar si estos enfoques se adaptan a su organización.

Además de implementar la ZT, SASE, SSE y soluciones reforzadas por hardware, las organizaciones creadoras animan encarecidamente a las entidades a aplicar las prácticas recomendadas que se enumeran a continuación. Estas prácticas recomendadas coinciden con los Objetivos de Desempeño en Ciberseguridad (CPG, por sus siglas en inglés) intersectoriales que desarrollaron la CISA y el NIST. Los CPG proporcionan un conjunto mínimo de prácticas y protecciones que la CISA y el NIST recomiendan que todas las organizaciones implementen.

Consulte los objetivos de desempeño en ciberseguridad intersectoriales de la CISA para obtener más información sobre los CPG y las prácticas de referencia recomendadas.

- **Implemente una solución de gestión centralizada.** Tener una gestión centralizada permite a los administradores de sistemas la capacidad de controlar el acceso remoto a aplicaciones y servidores, gestionar el acceso privilegiado y simplificar el control de la red. Sin la capacidad de implementar, monitorear y administrar a través de un punto centralizado, el costo asociado con el soporte técnico, la resolución de problemas de conexiones VPN y el soporte del cliente VPN aumenta. La capacidad de monitorear y gestionar el entorno VPN es fundamental para las defensas de la red moderna debido al problema subyacente de que ninguna VPN puede garantizar una seguridad absoluta. Además, si se produce una violación de datos debido a un error del usuario o de proveedores externos, una organización no puede probar fácilmente el origen del problema sin el acceso centralizado mencionado anteriormente a los datos que identifican al usuario, la aplicación o la conexión.[7]

- **Implemente la segmentación de red.** Todas las conexiones a la red de OT se niegan de forma predeterminada, a menos que se permitan explícitamente (p. ej., por dirección IP y puerto) para una funcionalidad específica del sistema [CPG 2.F]. Los límites deben ser unidireccionales para los sistemas más importantes, las comunicaciones y los sistemas de acceso remoto en general. Consulte el aviso conjunto La NSA y la CISA recomiendan acciones inmediatas para reducir la exposición en las tecnologías operativas y los sistemas de control para obtener más información.
- **Implemente la orquestación, automatización y respuesta de seguridad (SOAR, por sus siglas en inglés)** mediante la aplicación de una respuesta automatizada a ciertos eventos de seguridad.
- **Desarrolle, mantenga, actualice y explore periódicamente planes de respuesta a incidentes de ciberseguridad de IT y OT** tanto para escenarios y procedimientos comunes como específicos de la organización. Los planes de respuesta se actualizan dentro de un período de tiempo basado en el riesgo después de las lecciones aprendidas de cualquier ejercicio o simulacro [CPG 2.S].
- **Automatice y valide los análisis de vulnerabilidad en todos los activos empresariales públicos.** Aplique los controles compensatorios adecuados para evitar las formas comunes de mal uso y explotación. Deshabilite todas las aplicaciones del sistema operativo y los protocolos de red innecesarios en los activos públicos [CPG 2.W].
- **Utilice soluciones de ciberseguridad de alto rendimiento y probadas** para automatizar la detección de intentos de inicio de sesión fallidos [CPG 2.G].
- **Integre un sistema de detección de incidentes** para ayudar a priorizarlos [CPG 3.A]. Integre sistemas que bloqueen de inmediato el acceso a dispositivos comprometidos sospechosos de ser maliciosos y desconecten las conexiones establecidas a los sistemas.
- **Implemente el archivo security.txt** para permitir que los investigadores de seguridad envíen debilidades o vulnerabilidades descubiertas de manera oportuna. Todos los dominios web públicos deben tener un archivo `security.txt` que cumpla con las recomendaciones de la Solicitud de comentarios (RFC, por sus siglas en inglés) 9116 [CPG 4.C]. Las organizaciones también deben tener una política de divulgación de vulnerabilidades bien definida y respaldada por la organización, que respalde el `security.txt`.
- **Realice copias de seguridad de forma periódica de todos los sistemas que sean necesarios para las operaciones diarias.** Las copias de seguridad deberían almacenarse por separado de los sistemas de origen y probarse de forma recurrente, al menos una vez al año [CPG 2.R].
- **Realice capacitaciones anuales sobre conceptos básicos de seguridad** (como phishing, violación de correo electrónico empresarial, seguridad operacional básica, seguridad de contraseñas, etc.) obligatorias para todos los empleados y contratistas para fomentar una cultura interna de seguridad y conciencia cibernética [CPG 2.I].
- **Implemente una solución sólida de gestión de identidad y acceso** que verifique la identidad con autenticación multifactor (MFA, por sus siglas en inglés) resistente al phishing [CPG 2.H].
- Para los sistemas más importantes, **utilice tecnología unidireccional reforzada por hardware** para enviar datos forenses, de auditoría y otros datos de seguridad desde redes sensibles a sistemas de monitoreo de acceso y seguridad SOAR basados en IT o en la nube. Esta aplicación de hardware mitiga los ciberataques que pasan por la nube o Internet y regresan a redes protegidas mediante hardware unidireccional. [GPC 2.Q].
- **Permita el acceso según los principios del mínimo privilegio.** Los usuarios solo deben tener acceso a los recursos que necesiten en cada momento. Los usuarios y dispositivos deben ser identificados y verificados de manera estricta para cada solicitud de acceso [CPG 2.E].

- **Establezca una hoja de ruta de adopción y una estrategia de implementación.**Realice un intercambio de ideas sobre cómo SASE beneficia a su organización en función de los objetivos de SASE [CPG 5.A].
- **Diseñe una hoja de ruta SASE flexible** donde cada capacidad tenga un plan sólido detrás. Con SASE, esta estrategia consiste en combinar la IT con objetivos orientados al negocio. Cada organización debe aportar información sobre qué beneficios tiene SASE para sus necesidades comerciales [CPG 5.A].
- **Coloque la colaboración, las estrategias, las tecnologías y las aplicaciones en un entorno de prueba** antes de que estén completamente operativas con las soluciones SASE [CPG 2.S].
- **Implemente medidas de seguridad técnicas para proteger su organización, como Mail Transfer Agent Strict Transport Security (MTA-STS)**, que proporciona cifrado estricto al tráfico de correo enviado a un dominio. Utilice la autenticación basada en DNS de entidades nombradas (DANE, por sus siglas en inglés), que permite a los administradores de red vincular certificados de seguridad de la capa de transporte (TLS, por sus siglas en inglés) a nombres de dominio.[8]
- Para evitar que se explote todo el sistema y proteger la información confidencial, **solo otorgue acceso a usuarios remotos específicos en lo que respecta a la función del usuario dentro de la organización** [CPG 2.W].
- **Utilice FWaaS** para proteger los activos digitales de su organización contra amenazas basadas en la web [GPC 2.Q].
- Para aumentar la seguridad de la red, **utilice ZTNA para limitar el acceso y las aplicaciones de los usuarios** a través de un agente de confianza [CPG 2.X].

Las organizaciones deben hacer lo siguiente al realizar la transición de soluciones de VPN a SSE/SASE (teniendo en cuenta que la migración puede requerir una planificación adecuada y una implementación secuencial):

- Impedir el acceso al plano de control.
- Utilizar una interfaz de gestión dedicada.
- Parchear, generar y analizar la telemetría de red relacionada con la solución de VPN.
- Considerar autenticar previamente a los usuarios.
- Utilizar MFA.
- Controlar las versiones de la configuración en ejecución (es decir, buscar activamente cambios en la configuración del dispositivo).

Seguir estas prácticas recomendadas e iniciar una evaluación completa de la postura de seguridad de una organización puede ayudar de forma eficaz a las organizaciones a implementar soluciones SASE y SSE. Estas soluciones ayudan a las organizaciones a mejorar las capacidades de seguridad, acceder a los recursos de la nube de forma más segura y respaldar un enfoque más sólido para la seguridad de la red, al tiempo que garantizan el cumplimiento de los requisitos reglamentarios.

REFERENCIAS

[1] Explotación activa de dos vulnerabilidades de día cero en la VPN Ivanti Connect Secure | Volexity

[2] Los agentes de amenazas explotan múltiples vulnerabilidades en las puertas de enlace de seguridad de Ivanti Connect y Policy Secure | CISA

[3] #StopRansomware: los afiliados del ransomware LockBit 3.0 explotan la vulnerabilidad CVE 2023-4966 de Citrix Bleed | CISA

[4] Poner fin a la confusión entre confianza cero, SSE y SASE

[5] ¿Qué es SASE? Palo Alto Networks

[6] Segmentación 202: arquitecturas unidireccionales, Waterfall Security

[7] 7 riesgos de seguridad comunes de las VPN: el no tan bueno, el malo y el feo | Imprivata

[8] Guía de implementación: protección de dominios de correo electrónico (ITSP.40.065 v1.1), Canadian Centre for Cyber Security

RECURSOS

- CISA: Arquitectura de referencia técnica de seguridad en la nube versión 2
- CISA: Implementar MFA resistentes al phishing
- CISA: Conexiones de Internet Confiables (TIC)
- CISA: Modelo de madurez de confianza cero
- Guía de implementación: protección de dominios de correo electrónico (ITSP.40.065 v1.1)
- Orientación sobre la configuración segura de protocolos de red (ITSP.40.062)
- Gestión de dispositivos edge: cinco desafíos y recomendaciones al utilizar dispositivos edge

AGRADECIMIENTOS

Waterfall Security contribuyó a esta guía.

DESCARGO DE RESPONSABILIDAD

El Gobierno de los Estados Unidos, a través de la CISA del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés), y las organizaciones autoras, no respaldan ningún producto o servicio comercial. Cualquier referencia a productos, procesos o servicios comerciales específicas mediante marcas de servicio, marcas comerciales, fabricantes o de otro modo se proporciona con fines informativos y no constituye ni implica respaldo, recomendación o favoritismo por parte de la CISA, el DHS o las organizaciones autoras.